МАРИЙ ЭЛ РЕСПУБЛИКЫН ВИКТЕРЖЕ

ПУНЧАЛ

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МАРИЙ ЭЛ

ПОСТАНОВЛЕНИЕ

от 21 декабря 2015 г. № 715

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Республики Марий Эл, подведомственных им организациях

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Республики Марий Эл, подведомственных им организациях, Правительство Республики Марий Эл п о с т а н о в л я е т:

Утвердить прилагаемое Положение об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Республики Марий Эл, подведомственных им организациях.

Председатель Правительства Республики Марий Эл №1 Л.Маркелов

002064 ✻

УТВЕРЖДЕНО
постановлением Правительства
Республики Марий Эл
от 21 декабря 2015 г. № 715

П О Л О Ж Е Н И Е

об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Республики Марий Эл, подведомственных им организациях

I. Общие положения

1. Настоящее Положение разработано в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и определяет угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее - информационные системы) в органах исполнительной власти Республики Марий Эл, подведомственных им организациях.

Угрозы безопасности персональных данных, обрабатываемых в информационных системах, относящиеся к угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах в органах исполнительной власти, подведомственных им организациях (далее - актуальные угрозы безопасности информационных систем), предусмотренные разделом 4 настоящего Положения, подлежат адаптации в ходе разработки органами исполнительной власти, подведомственными им организациями частных моделей угроз безопасности персональных данных для каждой информационной системы.

При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик информационной системы, эксплуатируемой при осуществлении органом исполнительной власти полномочий или при осуществлении подведомственной ему организацией функций, а также

применяемых в ней информационных технологий и особенностей ее функционирования. По результатам анализа органом исполнительной власти, подведомственной ему организацией принимается решение об отнесении информационной системы к одному из видов информационных систем, приведенных в пункте 2 настоящего Положения.

В частной модели угроз безопасности информации указываются:

описание информационной системы и ее структурно-функциональных характеристик;

описание угроз безопасности информации с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, а также с учетом возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Актуальные угрозы безопасности персональных данных, обрабатываемых в информационных системах, относящиеся к актуальным угрозам безопасности информационных систем, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в информационных системах. Указанные изменения согласовываются Департаментом информатизации и связи Республики Марий Эл с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в соответствии с частью 7 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. В органах исполнительной власти создаются и эксплуатируются информационные системы. В зависимости от предназначения такие информационные системы подразделяются на:

а) информационные системы обеспечения типовой деятельности органов исполнительной власти Республики Марий Эл (далее - информационные системы обеспечения типовой деятельности) - информационные системы, предназначенные для автоматизации деятельности органов исполнительной власти в рамках исполнения ими полномочий, предусмотренных нормативными правовыми актами Российской Федерации и нормативными правовыми актами Республики Марий Эл, за исключением полномочий, автоматизация или информационная поддержка которых предусмотрена информационными системами специальной деятельности.

К информационным системам обеспечения типовой деятельности относятся: информационные системы управления персоналом, информационные системы управления финансами, информационные системы документооборота;

б) информационные системы обеспечения специальной

деятельности органов исполнительной власти Республики Марий Эл (далее - информационные системы обеспечения специальной деятельности) - информационные системы, предназначенные для автоматизации либо информационной поддержки предоставления государственных услуг и исполнения государственных функций, предусмотренных нормативными правовыми актами Республики Марий Эл.

К информационным системам обеспечения специальной деятельности относятся: государственная информационная система Республики Марий Эл «Система межведомственного электронного взаимодействия Республики Марий Эл», единая региональная автоматизированная информационная система поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг Республики Марий Эл «Полтава - Многофункциональный центр», информационные системы, применяемые для осуществления деятельности органов исполнительной власти.

II. Информационные системы обеспечения типовой деятельности

3. Информационные системы обеспечения типовой деятельности характеризуются тем, что в качестве объектов информатизации выступают автономные автоматизированные рабочие места или рабочие места локальных вычислительных сетей, имеющих или не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных в информационные системы обеспечения типовой деятельности осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные субъектов могут выводиться из информационных систем обеспечения типовой деятельности с целью передачи персональных данных третьим лицам как в электронном, так и в бумажном виде.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее - СКЗИ).

4. Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств.

Контролируемой зоной информационных систем являются здания и отдельные помещения, в которых ведется обработка и хранение персональных данных. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование информационной системы. Вне

контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

5. Информационные системы управления персоналом предназначены для персонального кадрового учета, управления кадровым резервом, проведения аттестации, повышения квалификации и для других целей, связанных с управлением персоналом.

В информационных системах управления персоналом обрабатывается обязательный перечень информации, имеющей характер персональных данных государственных гражданских служащих Республики Марий Эл и работников, граждан, подавших сведения для участия в конкурсе на замещение вакантных должностей государственной гражданской службы Республики Марий Эл и на включение в кадровый резерв, а также граждан, претендующих на замещение должностей руководителей подведомственных органам исполнительной власти организаций: фамилия, имя, отчество, дата и место рождения, адрес, паспортные данные, сведения для заполнения личного дела, личные карточки работников формы № Т-2, сведения из трудовой книжки, дополнительный перечень информации, имеющей характер персональных данных работников.

6. Информационные системы управления финансами предназначены для обработки персональных данных, необходимых для бухгалтерского и управленческого финансового учета, предоставления информации в органы Пенсионного фонда Российской Федерации и налоговые органы, систему обязательного медицинского страхования.

В информационных системах управления финансами обрабатываются следующие персональные данные государственных гражданских служащих Республики Марий Эл и работников: фамилия, имя, отчество, дата и место рождения, паспортные данные, адрес, номер телефона, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, табельный номер, должность, номер приказа и дата поступления на государственную гражданскую службу (увольнения), номер приказа и дата принятия на работу (увольнения) работников, номер лицевого счета для перечисления денежного содержания и иных выплат гражданских служащих и работников; фамилия, имя отчество, паспортные данные, адрес, должность, номер телефона (либо иной вид связи), идентификационный номер налогоплательщика, платежные реквизиты граждан, являющихся стороной государственного контракта.

7. Информационные системы документооборота предназначены для автоматизации делопроизводства, служебной переписки, архивной деятельности, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам.

В информационных системах документооборота обрабатываются: фамилия, имя, отчество, должность, контактные данные (электронный адрес, номер телефона), иная информация в документах, имеющая характер персональных данных.

III. Информационные системы обеспечения специальной деятельности

8. Информационные системы обеспечения специальной деятельности характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы и локальные информационные системы, имеющие или не имеющие подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных в информационные системы обеспечения специальной деятельности осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные субъектов персональных данных обрабатываются с целью получения государственных услуг и могут выводиться из информационных систем как в электронном, так и в бумажном виде.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием СКЗИ.

Контролируемой зоной информационных систем являются здания и отдельные помещения, в которых ведется обработка и хранение персональных данных. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование информационных систем. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

9. Государственная информационная система Республики Марий Эл «Система межведомственного электронного взаимодействия Республики Марий Эл», созданная в соответствии с постановлением Правительства Республики Марий Эл от 26 апреля 2012 г. № 137 «Об организации межведомственного информационного взаимодействия в Республике Марий Эл», предназначена для предоставления государственных услуг в электронной форме, межведомственного информационного взаимодействия в электронной форме, информационного взаимодействия в электронной форме с многофункциональными центрами предоставления государственных и муниципальных услуг, созданными в Республике Марий Эл.

Посредством использования информационной системы

обрабатываются (передаются) персональные данные заявителей, необходимые для предоставления государственных услуг и получаемые в соответствии с законодательством Российской Федерации в рамках межведомственного информационного взаимодействия, в том числе из базовых государственных информационных ресурсов.

10. Единая региональная автоматизированная информационная система поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг Республики Марий Эл «Полтава - Многофункциональный центр» предназначена для обработки персональных данных, предоставляемых заявителями, получаемых из базовых государственных информационных ресурсов, от государственных органов и организаций, используемых для подготовки ответов на запрос заявителя в соответствии с административными регламентами предоставления государственных услуг, утвержденными нормативными правовыми актами соответствующего органа исполнительной власти.

11. Информационные системы по направлениям деятельности органов исполнительной власти, исполняемым функциям предназначены для обеспечения деятельности органов исполнительной власти и исполнения функций, не предусмотренных пунктами 9 и 10 настоящего Положения.

В информационных системах обрабатываются персональные данные, необходимые для выполнения деятельности органов исполнительной власти, исполнения функций и предоставления государственных услуг, определенных в нормативных правовых актах Республики Марий Эл.

IV. Актуальные угрозы безопасности информационных систем

12. Угрозы безопасности персональных данных рассмотрены в Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра Федеральной службы безопасности Российской Федерации 31 марта 2015 г. № 149/7/2/6-432, и в Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.

Учитывая особенности обработки персональных данных в органах исполнительной власти, а также категорию и объем персональных данных, обрабатываемых в информационных системах, основными

характеристиками безопасности информации являются конфиденциальность, целостность и доступность.

Конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Целостность - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

13. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Основная часть угроз безопасности персональных данных в информационных системах органов исполнительной власти относятся к 3-му типу.

В информационных системах органов исполнительной власти и подведомственных им организаций при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена для защиты персональных данных применяются СКЗИ.

14. Основными актуальными угрозами безопасности персональных данных в информационных системах являются:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационным ресурсам информационных систем, включая пользователей информационных систем;

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационным системам, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

угрозы, возникновение которых напрямую зависит от свойств техники и программного обеспечения, используемого в информационных системах;

угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ.

15. Для определения актуальных угроз безопасности информационных систем обеспечения типовой деятельности принимаются во внимание следующие особенности:

использование стандартных (унифицированных) технических средств обработки информации;

использование типового программного обеспечения;

наличие незначительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

дублирование информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;

незначительные негативные последствия для субъектов персональных данных при реализации угроз безопасности информационных систем;

эксплуатация информационных систем органами исполнительной власти без привлечения на постоянной основе сторонних организаций;

жесткая регламентация процедуры взаимодействия со сторонними организациями;

наличие выходов в сети общего пользования.

16. Учитывая особенности информационных систем обеспечения типовой деятельности, изложенные в пункте 14 настоящего Положения, актуальными угрозами безопасности информационных систем обеспечения типовой деятельности в органах исполнительной власти являются:

угрозы локального внедрения вредоносных программ;

угрозы анализа сетевого трафика;
угрозы сканирования сети;
угрозы выявления паролей;
угрозы подмены доверенного объекта сети;
угрозы навязывания ложного маршрута сети;
угрозы внедрения ложного объекта сети;
угрозы типа «отказ в обслуживании»;
угрозы удаленного запуска приложений;
угрозы внедрения по сети вредоносных программ;
угрозы непреднамеренного или преднамеренного вывода из строя технических средств и средств защиты информации;
угрозы несанкционированного отключения средств защиты информации;
угрозы непреднамеренной модификации (уничтожения) информации пользователями;
угрозы надежности технических средств и коммуникационного оборудования;
угрозы достаточности и качества применяемых средств защиты информации;
угрозы самостоятельного создания способов атак, подготовки и проведения атак за пределами контролируемой зоны;
угрозы проведения атак при нахождении в пределах контролируемой зоны;
угрозы проведения атак на этапе эксплуатации СКЗИ на документацию на СКЗИ и компоненты среды функционирования СКЗИ;
угрозы проведения атак на этапе эксплуатации СКЗИ на помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - совокупность элементов систем обработки данных), на которых реализованы СКЗИ и среда функционирования СКЗИ;
угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;
угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений сведений о мерах по разграничению доступа в помещения, в которых находятся совокупности элементов систем обработки данных, на которых реализованы СКЗИ и среда функционирования СКЗИ;
угрозы использования штатных средств информационных систем,

ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

угрозы физического доступа к совокупности элементов систем обработки данных, на которых реализованы СКЗИ и среда функционирования СКЗИ;

угрозы воздействия на аппаратные компоненты СКЗИ и среду функционирования СКЗИ, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

17. Для определения актуальных угроз безопасности информационных систем обеспечения специальной деятельности принимаются во внимание следующие особенности:

использование широкой номенклатуры технических средств получения, отображения и обработки информации;

использование специального (адаптированного под конкретную задачу) программного обеспечения;

наличие значительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

построение информационной системы на базе распределенной по территории Республики Марий Эл вычислительной сети со сложной архитектурой;

наличие выходов в сети общего пользования;

использование разнообразной телекоммуникационной среды, принадлежащей различным операторам связи;

широкое применение средств защиты информации, включая сертифицированные СКЗИ;

использование аутсорсинга при создании и эксплуатации информационной системы и ее элементов;

сложность с дублированием больших массивов информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;

значительные негативные последствия при реализации угроз безопасности информационных систем;

недостаточная квалификация пользователей и обслуживающего информационные системы и средства защиты информации персонала.

18. Учитывая особенности информационных систем обеспечения специальной деятельности, изложенные в пункте 17 настоящего Положения, актуальными угрозами безопасности информационных систем обеспечения специальной деятельности в органах исполнительной власти являются:

угрозы локального внедрения вредоносных программ;

угрозы анализа сетевого трафика;

угрозы сканирования сети;
угрозы выявления паролей;
угрозы подмены доверенного объекта сети;
угрозы навязывания ложного маршрута сети;
угрозы внедрения ложного объекта сети;
угрозы типа «отказ в обслуживании»;
угрозы удаленного запуска приложений;
угрозы внедрения по сети вредоносных программ;
угрозы непреднамеренного или преднамеренного вывода из строя технических средств и средств защиты информации;
угрозы несанкционированного отключения средств защиты информации;
угрозы непреднамеренной модификации (уничтожения) информации пользователями;
угрозы надежности технических средств и коммуникационного оборудования;
угрозы достаточности и качества применяемых средств защиты информации;
угрозы нарушения работы аппаратных компонентов серверного оборудования с установленными компонентами виртуальной среды;
угрозы несанкционированного удаленного доступа к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера» на открытые сетевые порты сервера с гипервизором в случае возникновения в его программном обеспечении уязвимостей;
угрозы получения несанкционированного удаленного доступа к интерфейсу системы управления;
угрозы несанкционированного сетевого подключения к виртуальной машине;
угрозы самостоятельного создания способов атак, подготовки и проведения атак за пределами контролируемой зоны;
угрозы проведения атак при нахождении в пределах контролируемой зоны;
угрозы проведения атак на этапе эксплуатации СКЗИ на документацию на СКЗИ и компоненты среды функционирования СКЗИ;
угрозы проведения атак на этапе эксплуатации СКЗИ на помещения, в которых находится совокупность элементов систем обработки данных, на которых реализованы СКЗИ и среда функционирования СКЗИ;
угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы

информационной системы;

угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений сведений о мерах по разграничению доступа в помещения, в которых находятся совокупности элементов систем обработки данных, на которых реализованы СКЗИ и среда функционирования СКЗИ;

угрозы использования штатных средств информационной системы, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

угрозы физического доступа к совокупности элементов систем обработки данных, на которых реализованы СКЗИ и среда функционирования СКЗИ;

угрозы воздействия на аппаратные компоненты СКЗИ и среды функционирования СКЗИ, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.